Diss High School

E-Safety Policy

Reviewed Annually

Contents

Introduction 3

Core principles 3

The importance and benefits of Internet use 3

Ensuring that Internet use enhances learning 3

Student evaluation of Internet content 3

Email management 4

School website content management 4

Social networking 4

Managing emerging technologies 4

Authorisation for Internet access 4

Risk assessment 4

Content filtering 5

ICT system security 5

Staff, student and parental awareness 5

Limitation of Liability 5

Monitoring and the consequences of improper/unacceptable use 5

Appendix 1 7

Acceptable Use Policy - Students 7

Appendix 2 – 12

Acceptable Use Policy - Staff 12

Introduction

The curriculum requires students to learn how to locate, retrieve and exchange information using ICT. Teachers need to plan to integrate the use of communications technology such as web-based resources and email. ICT skills are vital to access life-long learning and employment.

Technologies present risks as well as benefits. Internet/social networking use for work, home, social and leisure activities is expanding in all sectors of society. This brings students into contact with a wide variety of influences, some of which may be unsuitable. Unmediated Internet access through computers, telephones, iPads etc. brings with it the possibility of placing students in embarrassing, inappropriate and even dangerous situations which could lead to safeguarding issues.

Core principles

- Guided educational use – curriculum Internet use should be planned, task-orientated and educational within a regulated and managed environment.
- Risk assessment – students must be protected from danger (violence, racism, exploitation) and learn how to recognise and avoid it.
- Responsibility – staff, governors, external providers, parents and students must take responsibility for the use of the Internet.
- Regulation – in some cases, eg unmoderated chat rooms, immediate dangers are presented and their use is banned. In most cases strategies for Internet access should be selected and developed to suit the educational activities, and their effectiveness monitored.
- This policy is based on the information provided in *Keeping Children Safe In Education – statutory guidance to schools and colleges (DfE)*
- With regard to radicalisation via the internet and social media the school adopts *The Prevent Duty – departmental advice for schools and childcare providers (DfE)*

The importance and benefits of Internet use

- Raise educational standards, promote pupil achievement
- Support the work of staff and enhance management systems
- Part of the curriculum and a necessary tool in teaching and learning
- Students are entitled to quality Internet access as part of their learning experience
- Access to worldwide resources and experts
- Educational and cultural exchanges between students worldwide
- Facilitate staff professional development
- Communication with external services
- Exchange of curriculum and administrative data

Ensuring that Internet use enhances learning

- Internet access will be designed expressly for student use and will include filtering appropriate to students' ages
- Students will be taught what is acceptable and what is not, and given clear learning objectives when using the Internet
- Internet use will be planned to enhance and enrich learning. Access levels and online activities will be provided and reviewed to ensure they reflect curriculum requirements and student age
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Student evaluation of Internet content

- Any user discovering unsuitable sites should report the address and content to the ICT technical support team, a teacher, or the designated Child Protection coordinator as appropriate

- The use of Internet derived materials must comply with copyright law
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
- Students will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work

Email management

- Pupils may only use approved email accounts on the school system
- Pupils should tell a member of staff if they receive offensive email
- Pupils should not reveal details such as address or telephone number of themselves or others or arrange to meet anyone in email communication
- Social messaging can interfere with learning and will be restricted
- Email sent to an external organisation should be carefully written and authorised by a teacher before sending

School website content management

- The point of contact on the website should be the school address, email and telephone number. Staff and students' home information will not be published
- Use of photographs showing students and students' names will not be used on the website without parental consent
- The School Administrator will take overall editorial responsibility and ensure that content is accurate and appropriate
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained

Social networking

- Students will not be allowed access to public or unregulated chat rooms, social networking sites and forums
- Students may only use regulated chat environments and forums – this use will be supervised, whenever possible, and the importance of chat room safety emphasised

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school
- Mobile phones will not be used by students
- The school's video cameras may be used by students for educational use under staff supervision only

Authorisation for Internet access

- Internet access is subject to monitoring by the ICT technical support team
- All staff and students (and students' parents) must sign the Acceptable Use Policy
- Inappropriate use of the Internet will be dealt with in accordance with the school's Behaviour Policy

Risk assessment

- Some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure such material is not accessed by students. However, it is not possible to guarantee that such material will never appear on a school computer – Diss High School cannot accept liability for material accessed or any consequences of Internet access
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- Methods to identify, assess and minimise risk will be reviewed regularly

Content filtering

- The school will work in partnership with parents, the DFE and the Internet Service Provider to ensure systems to protect students are reviewed and improved
- Any Internet user should report unsuitable/illegal sites to the ICT technical support team
- The ICT Department will oversee regular checks to ensure that the filtering methods used are appropriate, effective and reasonable. Content is currently filtered using "Netsweeper".
- If filtered websites need to be used by staff, they may request ICT technical support to have them unblocked for a set period of time

ICT system security

- The school's ICT systems will be reviewed regularly with regard to security
- Virus protection will be installed and updated regularly
- Files held on the school's network will be regularly checked
- Use of portable media such as memory sticks and DVDs will be reviewed regularly
- Downloading of unauthorised files will be prohibited, and where possible blocked
- Use of the school's ICT systems will be subject to the Data Protection Act and the Computer Misuse Act

Staff, student and parental awareness

- All stakeholders will be made aware of this policy and how it relates to them
- All students will sign the Acceptable Use Policy – countersigned by parents **Appendix 1**
- All staff will sign the Acceptable Use Policy **Appendix 2**
- Rules for responsible computer and Internet Use will be made available on student desktops
- Students will be instructed in responsible and safe Internet use before being granted access
- Responsible use of the Internet, including social networking will be discussed through PSHEE and ICT lessons, covering use both within and outside school
- Staff training in safe and responsible Internet use and on the contents of this policy will be provided as required
- A partnership approach with parents will be encouraged, with relevant information on issues covered by this policy made available
- Cases of Internet misuse and other disciplinary breaches related to the policy will be dealt with through the school's Behaviour, Bullying and Safeguarding/Child Protection Policies, as appropriate. In cases of potential radicalisation/extremism The Prevent Duty will be implemented and could involve referral of individuals to the Prevent Duty Delivery Board and the Channel Panel (after consultation with KSCB and Police)
- Any complaints associated with the application of this policy will be dealt with through the school's usual complaints procedure.

Limitation of Liability

- Diss High School will not be responsible for damage/harm to persons, files, data, or hardware.
- While Diss High School employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.
- Diss High School will not be responsible, financially or otherwise, for unauthorised transactions conducted over the school network.
- Violations of this policy may have disciplinary repercussions, including:
    - Suspension of network, technology, or computer privileges
    - Legal action and/or prosecution

Monitoring and the consequences of improper/unacceptable use

- The School exercises its right to monitor an employee's use of information systems and internet access. Monitoring will take place where the school believes unauthorised use of the information

system may be taking place, or the system may be being used for criminal purposes, or for storing unauthorised text, imagery or sound. This policy informs employees of what monitoring may take place and the reasons for it.

- Where an incident, as described above, occurs the school should contact Educator Solutions HR Services in the first instance. This is to ensure that various legal requirements are adhered to.
- Under data protection law this type of monitoring is called 'occasional monitoring'. This is where the employer introduces monitoring as a short term measure to address a particular issue e.g. performance or conduct where concerns are of the nature explained above. Where monitoring takes place schools must have due regard to article 8 of the European Convention on Human Rights, which means the employee still has a right to privacy in the workplace. Therefore, the school should carry out an impact assessment before undertaking any monitoring. This will help to determine whether monitoring is a proportionate response to the issue and therefore lawful. The ICO's employment practices guide provides an outline impact assessment on page 59-64 of its guidance.
    - Systematic monitoring: E-safety monitors in schools, using an nsix email address, automatically receive a copy of any emails sent or received by nsix accounts at the school which are flagged as a potential safety concern. Academies may have different automatic monitoring in place. For advice regarding this type of monitoring please speak with the school/academy's ICT provider.

- Employees must be aware that improper or unacceptable use of the internet or email systems could result in the use of the school's Disciplinary Procedure and, in some cases, legal proceedings. Sanctions will depend upon the gravity of misuse and could result in summary dismissal in some cases.
- This policy relies on employees acting responsibly and in accordance with the outlined restrictions. Where employees have concerns that a colleague is acting in breach of the outlined restrictions, they are encouraged to raise this with the Headteacher or Chair of Governors if the concerns relate to the Headteacher.
- If the concern involves possible inappropriate interaction between a colleague and a pupil, referral may be made to the designated senior professional in the school.

This policy should be read in conjunction with and have due regard to the School's Internet, Social Networking and email Use Policy

Appendix 1.

Acceptable Use Policy - Students

Introduction

This Acceptable Use Policy outlines the guidelines and behaviours that users are expected to follow when using school technologies or when using personally-owned devices on the school site.

- The Diss High School network is intended for educational purposes.
- All activity over the network or using the school's technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies.
- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- Diss High School makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the school network or other technologies are expected to alert IT support immediately of any concerns for safety or security.

Technologies Covered

Diss High School may provide Internet access, desktop computers, mobile computers or devices, online collaboration capabilities, message boards, email, and more.

As new technologies emerge, Diss High School will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the school are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

Diss High School provides its users with access to the Internet, including websites, resources, content, and online tools. That access will be restricted in compliance with school policies. Web browsing may be monitored and web activity records kept.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow school protocol to alert IT Support or submit the site for review.

Email

Diss High School may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.

The school will provide users with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the school policy or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

the use of third party e-mail accounts (i.e. Hotmail, Google mail and Yahoo Mail) is not permitted.

Social / Collaborative Content

Recognising the benefits collaboration brings to education, Diss High School may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices Policy

Diss High School may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with care; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to IT support immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices off the school network may be monitored.

Personally Owned Devices Policy

Students should keep personally-owned devices (including laptops, tablets and smart phones) turned off and put away during school hours—unless in the event of an emergency or as instructed by a teacher or staff for educational purposes.

Because of security concerns, when personally-owned mobile devices are used on site, they should not be used over the school network without express permission from IT support. In some cases, a separate network may be provided for personally-owned devices.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Users must use only their own credentials to access school systems or credentials given to them by IT Support. They must not share their username / password with others.

Downloads / Uploads

Users should not download or attempt to download or run any programs over the school network or onto school resources without express permission from IT support.

You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, and only for education purposes.

Any sensitive information transmitted or taken off site must be encrypted and only sent by authorised personnel.

Etiquette Online

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognise that amongst the valuable content online, there is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there and can sometimes be shared and spread in ways you never intended.

Plagiarism

Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, birthday, or financial information, over the Internet without adult permission. Users should recognise that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Examples of Acceptable Use

I will:

- ✓ Use school technologies for school-related activities.
- ✓ Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- ✓ Treat school resources carefully, and alert staff if there is any problem with their operation.
- ✓ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- ✓ Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (i.e. images, messages, posts) online.
- ✓ Use school technologies at appropriate times, in approved places, for educational pursuits.
- ✓ Cite sources when using online sites and resources for research.
- ✓ Recognise that use of school technologies is a privilege and treat it as such.
- ✓ Be cautious to protect the safety of myself and others.
- ✓ Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use

I will **not**:

- ✗ Use school technologies in a way that could be personally or physically harmful.
- ✗ Attempt to find inappropriate images or content.
- ✗ Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- ✗ Try to find ways to circumvent the school's safety measures and filtering tools.
- ✗ Use school technologies to send spam or chain mail.
- ✗ Plagiarise content I find online.
- ✗ Post personally identifying information, about myself or others.
- ✗ Agree to meet someone I meet online in real life.
- ✗ Use language online that would be unacceptable in the classroom.
- ✗ Use school technologies for illegal activities or to pursue information on such activities.
- ✗ Attempt to hack or access sites, servers, or content that isn't intended for my use.
- ✗ Give out my username and/or password to others, or try to access Schools' systems with another person's account.

*This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.***Limitation of Liability**

Diss High School will not be responsible for damage or harm to persons, files, data, or hardware.

While Diss High School employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

Diss High School will not be responsible, financially or otherwise, for unauthorised transactions conducted over the school network.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or exclusion from school and school-related activities
- Legal action and/or prosecution

I have read and understood this Acceptable Use Policy and agree to abide by it:

.....

(Student Printed Name)

....

....

(Student Signature) (Date)

I have read and discussed this Acceptable Use Policy with my child:

.....

(Parent/Carer Printed Name)

....

....

(Parent/Carer Signature) (Date)

Appendix 2 –

Acceptable Use Policy - Staff

All staff are expected to abide by the guidelines and behaviours below when using school technologies or when using personally-owned devices on the school site.

- The Diss High School network is intended for educational/work purposes.
- All activity over the network or using the school's technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies.
- Misuse of school resources can result in disciplinary action.
- Users of the school network or other technologies are expected to alert IT support immediately of any concerns for safety or security.

Technologies Covered

- Diss High School may provide Internet access, desktop computers, mobile computers or devices, video conferencing capabilities, online collaboration capabilities, message boards, email, and more.
- As new technologies emerge, Diss High School will attempt to provide access to them. The policies outlined in this document are intended to cover ***all*** available technologies, not just those specifically listed.

Usage Policies

- All technologies provided by the school are intended for education/work purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access

- Diss High School provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with school policies.
- Web access is not for personal use unless with permission from the Headteacher.
- Web browsing may be monitored and web activity records may be kept.
- Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow school protocol to alert IT Support or submit the site for review.

Email

- email can only be accessed through Diss High School approved email accounts.
- Diss High School may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.
- The school will provide users with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the school policy.
- Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.
- email communication is subject to data protection law. When sending emails to more than one person, BCC all recipients so that their data is not shared.

Social / Collaborative Content

- Recognising the benefits collaboration brings to education, Diss High School may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.
- Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.
- Anyone under contract and working in education needs to ensure, both for the school's safety and their own, that activity on social networking sites:
  - does not bring the school into disrepute
  - does not bring the teacher into disrepute
  - does not expose the school to legal liability
  - reflects 'safer internet' practices
  - minimises risks associated with the personal use of social media by professionals and reflects the school's standard of behaviour and staff code of conduct.
- Be professional on the internet - including Facebook, Twitter and any other social media networks.
  - Don't post anything inappropriate, including comments or photos which might embarrass yourself or the school.
  - Avoid interacting with, initiating contact with or "friending" current (and recent) pupils using your personal profile.
  - Keep all school-related conversations focused on school, teaching and learning.
  - Remember, there is potential for anything you post online to be copied and distributed. Bear this in mind every time you post.
  - Check:
    - your privacy settings
    - predictive text
    - Are you able to delete the content once you have posted it?
    - How long will the material stay online?
- Consider your digital footprint
- If you feel you are a victim of cyberbullying you should report it via the appropriate channels

Mobile Devices Policy

- Diss High School may provide users with mobile computers or other devices. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network. Anything stored on the local Hard Drive will not be backed up by the network and you will need to keep copies if needed.
- Where required, drives on mobile devices may be encrypted to keep data secure. Passwords must not be written down or given to anyone else (apart from IT Support if required). If you forget the password the data held on the device will be lost.
- Users should report any loss, damage, or malfunction to IT support immediately. Users or departments may be financially accountable for any damage resulting from negligence or misuse.
- The devices battery must be looked after as it cannot be guaranteed to be replaced. It needs to be fully discharged regularly and charged back to 100%. Heat dramatically decreases battery and device life. When used do not place in situations where it could overheat (e.g. covering vents, placing on fabrics, etc.).
- If extra software is installed on the mobile device, you must have a valid licence to do this. Please consult IT Support if you are unsure. Use of school-issued mobile devices off the school network may be monitored and/or filtered.
- Devices must be returned to IT Support if you cease employment of Diss High School for a temporary period of time or leave permanently. Devices may also be requested to be returned if not being used appropriately.

Security

- Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.
- If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.
- Users must use only their own credentials to access school systems or credentials given to them by IT Support. They must not share their username / password with others.
- Devices must not be left unattended when logged on, as other people may gain access to sensitive information (e.g. SIMS .net, SIMS Learning Gateway, OPGS Portal). Devices must be locked or logged off when unattended to prevent unauthorised access.

Downloads / Uploads

- Users should not download or attempt to download or run any programs over the school network or onto school resources without express permission from IT support.
- You may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, and only for education purposes.
- Any sensitive information transmitted or taken off site must be encrypted and only sent by authorised personnel.

Etiquette Online

- Users should always use the Internet, network resources, and online sites in a courteous and respectful manner. Users should also recognise that amongst the valuable content online, there is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.
- Users should also remember not to post anything online that they wouldn't want students, parents, colleagues, or future employers to see. Once something is online, it's out there and can sometimes be shared and spread in ways you never intended.

Plagiarism

- Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.